Pseudorandom operators of the circular ensembles

Yaakov S. Weinstein* and C. Stephen Hellberg†
Center for Computational Materials Science, Naval Research Laboratory, Washington, D.C. 20375, USA

(Received 8 July 2004; published 28 January 2005; corrected 29 March 2005)

We demonstrate quantum algorithms to implement pseudorandom operators that closely reproduce statistical properties of random matrices from the three universal classes: unitary, symmetric, and symplectic. Modified versions of the algorithms are introduced for the less experimentally challenging quantum cellular automata. For implementing pseudorandom symplectic operators we provide gate sequences for the unitary part of the time-reversal operator.

DOI: 10.1103/PhysRevA.71.014303 PACS number(s): 03.67.Lx, 02.10.Yn

The possibility of manipulating, transferring, and storing information in a way that preserves quantum coherence has led to a reexamination and extension of the postulates of information processing [1]. This field of study, known as quantum information processing, can claim as triumphs the discovery of quantum algorithms that factor large numbers [2], search databases quickly [3], and simulate quantum systems efficiently [4]. In addition, powerful communication and cryptographic protocols have been suggested based on the laws of quantum mechanics [1].

Generation of random numbers is a basic component of classical information theory. Their quantum counterparts, random quantum states and operators, likewise play a vital role in quantum information theory. Quantum communication protocols utilizing randomness include saturation of the classical communication capacity of a noisy quantum channel by random states [5] and superdense coding of quantum states via random operators [6]. Quantum computing protocols facilitated by random unitaries include quantum process tomography via a random operator fidelity decay experiment to identify types and strengths of noise generators [7]. In addition, the amount of multipartite entanglement in random states approaches the maximum at a rate exponential with the number of qubits in the system [8].

Random quantum states, generated by applying a random operator to computational basis state, can also be used for unbiased sampling. When testing an algorithm, such as quantum teleportation, or a communications scheme it is desirable to insure success for all possible quantum states. This can be done via quantum process tomography, however this is extremely inefficient [9]. Rather, one could test the likelihood of success with states drawn in an unbiased manner from the space of all quantum states, similar to sampling statistics in other contexts.

To capitalize on the above uses of random states and operators, it is necessary to efficiently implement random matrices on a quantum computer. This would appear to be a daunting task considering that the number of independent variables in a given random operator grows exponentially with matrix dimension. Nevertheless, pseudorandom operators suggest that it may be possible to efficiently reproduce statistical properties of randomness on a quantum computer [7]. In this paper we extend the algorithm of Ref. [7] to produce pseudorandom operators from the universal random matrix classes with time-reversal symmetry.

Pseudorandom operators from the universal classes with time-reversal symmetry may help a quantum computer simulate systems with time-reversal symmetries. These systems are especially important in the areas of quantum chaos [10] and decoherence [11], where the physical system or environment to be studied tend to be modeled with time-reversal symmetry. We note that models of decoherence, specifically with random classical fields, have already been implemented on a nuclear magnetic resonance quantum information processor [12].

In addition, we extend our recent work [13] and show that random operators from all three universal classes can be implemented on the less experimentally challenging quantum cellular automata (QCA) architecture. This further demonstrates the usefulness of a QCA in the study of complex quantum evolution. For both architectures we show how to implement the unitary part of the time-reversal operator on a quantum computer which, for the QCA case, requires identifying a suitable, nonstandard form of the time-reversal operator.

Random matrices were first introduced by Wigner to describe the energy level spacings of large nuclei [14]. Since then, random matrices have functioned as a universal model for a host of complex systems ranging from quantum dots to field theory [15]. The circular ensembles of unitary matrices were introduced by Dyson [16] as alternatives to the Gaussian ensembles of Hermitian matrices [14,17]. The three circular ensembles are the circular unitary ensemble (CUE) of arbitrary unitary matrices, appropriate for modeling systems without time reversal symmetry, the circular orthogonal ensemble (COE) of symmetric unitary matrices, appropriate for systems having time-reversal invariance and integral spin or rotational symmetry, and the circular symplectic ensemble (CSE) of self-dual unitary quaternion matrices, appropriate for systems with time-reversal invariance, half-integer spin, and no rotational symmetries. Each universality class has properties unique unto itself. For example, the degree of level repulsion (the rate of change of nearest neighbor eigenangle spacings as the spacing goes to zero) is $P(s) \sim s$ for

*Author to whom correspondence should be addressed. Electronic address: weinstei@dave.nrl.navy.mil

†Electronic address: hellberg@dave.nrl.navy.mil

the COE, $P(s) \sim s^2$ for the CUE, and $P(s) \sim s^4$ for the CSE, where s is the nearest neighbor eigenangle spacing. Additionally, the distribution of eigenvector component amplitudes follow the χ^2_ν distribution [18]

$$P_\nu(y) = \frac{\nu/2^{(\nu/2)}}{\Gamma(\nu/2)\langle y\rangle}\left(\frac{y}{\langle y\rangle}\right)^{\nu/2-1}\exp\left(\frac{\nu y}{2\langle y\rangle}\right), \tag{1}$$

where y is the eigenvector component amplitude, and $\langle y\rangle$ is the mean value of y. The number of degrees of freedom, ν, is 1 for the orthogonal ensemble, 2 for the unitary ensemble, and 4 for the symplectic ensemble.

The algorithm introduced in [7] to produce pseudorandom operators of arbitrary unitaries, the CUE, consists of m iterations of the n-qubit gate: apply a random SU(2) rotation to each qubit, then evolve the system via all nearest neighbor couplings [7]. A random SU(2) rotation on qubit j of iteration i is defined as [18]

$$R(\theta_i^j, \phi_i^j, \psi_i^j) = \begin{pmatrix} e^{i\phi_i^j}\cos\theta_i^j & e^{i\psi_i^j}\sin\theta_i^j \\ -e^{-i\psi_i^j}\sin\theta_i^j & e^{-i\phi_i^j}\cos\theta_i^j \end{pmatrix}, \tag{2}$$

where the angles ϕ_i^j, and ψ_i^j are drawn uniformly from the intervals

$$0 \leqslant \phi_i^j \leqslant 2\pi, \quad 0 \leqslant \psi_i^j \leqslant 2\pi, \tag{3}$$

and $\theta_i^j = \sin^{-1}(\xi_i^{j\,1/2})$ where ξ_i^j is drawn uniformly from 0 to 1. The nearest neighbor coupling operator at every iteration is

$$U_{NNC} = \exp\left(i(\pi/4)\sum_{j=1}^{n-1}\sigma_z^j \otimes \sigma_z^{j+1}\right), \tag{4}$$

where σ_z^j is the z-direction Pauli spin operator. The random rotations are different for each qubit and each iteration, but the coupling constant is always $\pi/4$ to maximize entanglement. After the m iterations, a final set of random rotations is applied. This algorithm has been shown, for up to ten qubits, to implement operators with statistical properties extremely close to those expected of the CUE [7] with relatively few iterations [19] (Fig. 1).

Random operators from the other two universal classes can be constructed from CUE operators. The goal of this paper is to demonstrate that these constructions allow for simple modifications of the pseudorandom algorithm described above to generate pseudorandom operators from these classes. To draw a matrix U_{COE} from the space of all the COE's simply draw U_{CUE} from the CUE's and multiply it by its transpose [17,18],

$$U_{COE} = U_{CUE}^T U_{CUE}. \tag{5}$$

Pseudorandom generation of such an operator is readily done. First, implement the CUE matrix U_{CUE} as above, retaining in memory (quantum or classical) the values of the $3n(m+1)+1$ independent variables necessary to implement the operator, three for each rotation of n qubits for $m+1$ rotations, and one for the coupling strength. Next, implement the transpose of the operator by applying the transpose of each specific operation in reverse order of the original U_{CUE} generation. To implement the transpose of the rotations apply the transpose of each individual qubit rotations. The transpose of the coupling operation is the same coupling $U_{NNC}^T = U_{NNC}$. In Fig. 2 we demonstrate that for eight qubits and 60 iterations the pseudorandom COE matrices generated in this way satisfy statistics of randomness by comparing the distributions $P(s)$ and $P(y)$ to that expected for the COE.

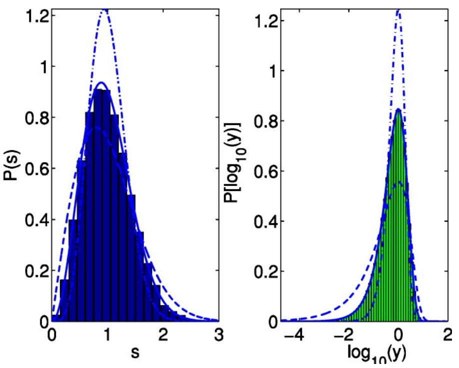

FIG. 1. Distributions of nearest neighbor eigenangle spacings s (left), and eigenvector component amplitudes y (right), for 100 realizations of eight-qubit, 60-iteration pseudorandom CUE operators compared to those expected for random unitaries of the COE (dash), CUE (solid), and CSE (dash-dot). The nearest neighbor eigenangle spacing distribution compares extremely well with the expected distribution $P_{CUE}(s) = (32s^2/\pi^2)\exp(-4s^2/\pi)$ and the operators' eigenvector component amplitude distribution almost exactly follows $P_{CUE}(y) = \exp(-y)$, which is appropriate when $\langle y\rangle = 1$ and in the limit $N \rightarrow \infty$.

We now turn to the symplectic ensemble, representing systems with half-integer spin that are invariant under time reversal. Following Mehta [17] we define the antiunitary time-reversal operator $T = ZC$, where C takes the complex conjugate and Z is unitary. The symplectic ensemble is characterized by an antisymmetric Z, i.e., $ZZ^* = -1$ where the asterisk means the non-Hermitian conjugate. We choose the representation such that Z is written $I_1 \otimes I_2 \otimes \cdots \otimes I_{n-1} \otimes z_n$ where I_j is the two-dimensional identity matrix and

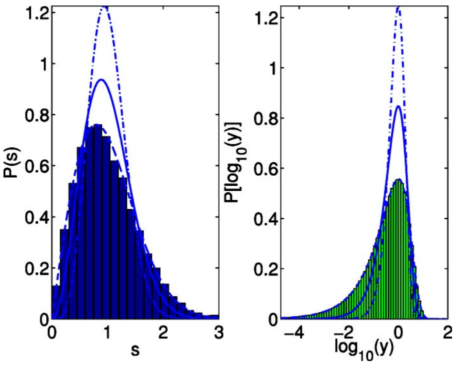

FIG. 2. Distributions of nearest neighbor eigenangle spacings s (left), and eigenvector component amplitudes y (right), for 100 realizations of eight-qubit, 60-iteration pseudorandom COE operators. The nearest neighbor eigenangle distribution compares very well with the distribution $P_{COE}(s) = (\pi s/2)\exp(-\pi s^2/4)$ and the eigenvector component amplitude distribution almost exactly follows $P_{COE}(y) = (1/\sqrt{2\pi y})\exp(-y/2)$.

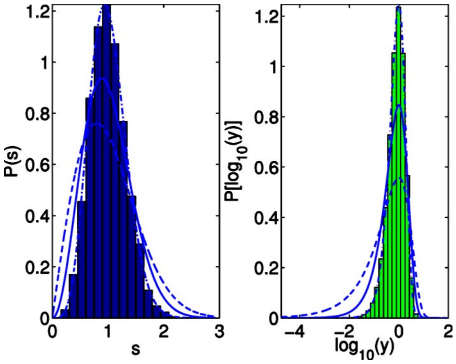

FIG. 3. Distributions of nearest neighbor eigenangles s (left) and eigenvector component amplitudes y (right), for 100 realizations of eight-qubit, 60-iteration pseudorandom CSE operators. The nearest neighbor eigenangle distribution compares very well with the distribution $P_{CSE}(s)=(64/9\pi)^3s^4\exp(-64s^2/9\pi)$ and the eigenvector component amplitude distribution almost exactly follows $P_{CSE}(y)=4y\exp(-2y)$.

$$z_j=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}. \quad (6)$$

In this way, a symplectic unitary is defined by

$$U^R_{CSE}\equiv -ZU^T_{CSE}Z=U_{CSE}. \quad (7)$$

and $U_{CSE}Z$ is antisymmetric unitary.

As with the COE operators, drawing an operator from the CSE can be done via CUE operators: draw U_{CUE} and multiply by its time reversal [17,20]

$$U_{CSE}=U^R_{CUE}U_{CUE}, \quad (8)$$

where $U^R_{CUE}=-ZU^T_{CUE}Z$. Using this construction pseudorandom CSE operators can be generated as follows: run the pseudorandom operator algorithm to implement U_{CUE}, apply Z via two rotations of the least significant qubit $z=\exp[-i(\pi/2)\sigma_z]\exp[-i(\pi/2)\sigma_x]$, where the σ_i are the Pauli matrices, U^T_{CUE} is implemented as explained in the COE case, apply Z. The negative sign is a global phase.

Figure 3 shows the eigenangle and eigenvector element distributions for CSE pseudorandom operators. We note that matrices of the CSE exhibit Kramers' degeneracy so we digress to explain how the above distributions are determined. Kramers' degeneracy allows the following basis choice for CSE matrices [10]:

$$|1\rangle, T|1\rangle, |2\rangle, T|2\rangle, \ldots, |N/2\rangle, T|N/2\rangle, \quad (9)$$

where T is the time-reversal operator. The nearest neighbor eigenangle distribution uses only one of each degenerate eigenangle. The eigenvectors corresponding to the degenerate eigenangles can be written as

$$|e_1\rangle = c_1|1\rangle + \tilde{c}_1T|1\rangle + c_2|2\rangle + \tilde{c}_2T|2\rangle\cdots,$$

$$T|e_1\rangle = -\tilde{c}^*_1|1\rangle + c^*_1T|1\rangle - \tilde{c}^*_2|2\rangle + c^*_2T|2\rangle\cdots. \quad (10)$$

Any given diagonalization code will not necessarily output the above form for the two eigenvectors of a degenerate eigenvalue, but superpositions of the two. Thus, as an invariant quantity to characterize the eigenvectors we use $y=|c_1|^2+|\tilde{c}_1|^2$ [10]. Using the above procedures, the distribution of nearest neighbor eigenangle and eigenvector components for the generated pseudorandom CSE operators are those shown in Fig. 3.

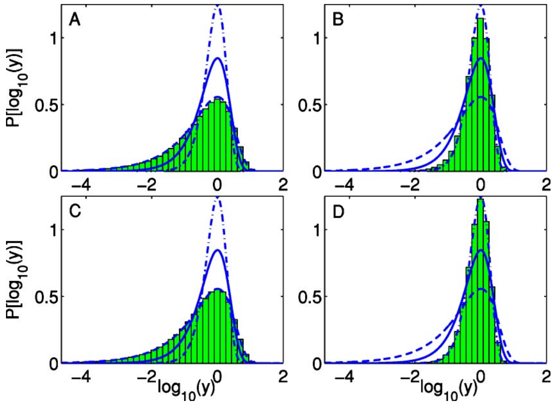

FIG. 4. Distributions of eigenvector component amplitudes y for quantum cellular automata (QCA) based operators: (a) 100 realizations of eight-qubit one-species COE, (b) 200 realizations of seven-qubit one-species CSE, (c) 100 realizations of eight-qubit two-species COE, and (d) 200 realizations of seven-qubit two-species CSE. All distributions are for $m=40$ iterations. The distributions of the two-species QCA operators are indistinguishable from those of random COE and CSE matrices. However, the one-species QCA operator distributions deviate from the random distributions due to mirror symmetry. We note that this symmetry would be broken in any actual experimental implementation due to unequal nearest neighbor couplings.

Classical cellular automata have been used to simulate many complex classical systems from crystal growth to fluid flow [21]. Thus, one may expect that quantum cellular automata can be used to model complex quantum systems. Reference [13] demonstrates the implementation of CUE pseudorandom operators. Here we extend that work to the other two random matrix classes.

A QCA system is devised of k species of qubits in which all qubits of a species are addressed simultaneously and equivalently. Experimental flexibility is a primary motivation to explore implementations via QCA. Removing the need for localized external Hamiltonians can greatly ease hardware specifications for actual implementations of quantum information processing. A number of works have been devoted to exploring the universality of QCA architectures [22–24] but, despite the greater experimental ease of QCA, relatively little work has been done to exploit the uniqueness of the QCA architecture [13,25].

Previous work has shown that the pseudorandom algorithm applied to a one-species QCA chain, such that all qubits undergo the same rotations, yields operators with eigenvalue and eigenvector distributions appropriate for CUE-type operators with mirror symmetries [13]. The use of a two-species QCA with alternating qubit species or the change of one nearest neighbor coupling constant (say from $\pi/4$ to $\pi/5$) is sufficient to break this symmetry.

For a QCA COE pseudorandom operator, one applies the pseudorandom operator algorithm, with all qubits of a species undergoing the same rotation, followed by its transpose, just as in the circuit architecture. The eigenvector component amplitude distribution for eight-qubit, one- and two-species COE operators is shown in Fig. 4.

To generate CSE pseudorandom operators requires the implementation of Z which above was done by individually addressing the least significant qubit. This operation is illegal on a QCA system. Thus, we must find an appropriate nonstandard representation of Z which allows all qubits of a species to be addressed equivalently.

To find a representation of Z amenable to a QCA implementation, we recall that for a symplectic matrix U_{CSE} the matrix $A=U_{CSE}Z$ is antisymmetric unitary. For every antisymmetric unitary matrix there exists a unitary matrix W such that $A=WZW^T$ [17]. We define our modified operator as $Z'=VZV^T$. Since $Z'Z'^{*}=-1$, by definition of a symplectic matrix, $(V^*)^T V=V(V^*)^T=\pm 1$. Thus, V must be a symmetric or antisymmetric unitary. We can then define the antisymmetric unitary $A'=U_{CSE}Z'=W'Z'W'^T$ and, following Mehta [17], we choose the unitary $U_{CUE}=(Z'W')^T$ and generate symplectic matrices via $U_{CSE}=-Z'U_{CUE}^T Z'U$. An example of a symmetric unitary operator, V, that allows the generation of CSE operators in the above fashion is the swap gate. This should not be surprising as the ordering of qubits is completely arbitrary. An operator Z' that is appropriate for our purposes is the rotation z applied to an odd number of qubits. Using this form of Z', pseudorandom symplectic operators (with mirror symmetry if all coupling constants are equal) can be implemented on a one-species QCA if there are an odd number of qubits. Similarly, two-species QCA implementations of pseudorandom symplectic operators can be achieved if one of the species consists of an odd number of qubits. The eigenvector component amplitude distribution of seven-qubit one- and two-species QCA operators is shown in Fig. 4.

In conclusion, we have demonstrated quantum algorithms for pseudorandom operators from the COE and CSE universal classes. As with the original CUE pseudorandom operators [7], we provide evidence that suggests that these operators may be able to satisfy statistical properties of these ensembles with an efficient number of gates. Efficient performance of such operators could be useful in simulating various complex quantum systems. Similar operators can also be implemented using the less experimentally demanding QCA. This is a further demonstration that a QCA system can be a useful tool in the study of randomness.

The authors would like to thank F. Haake for clarification of the CSE eigenvector component statistics and Al. L. Efros for insightful comments. The authors acknowledge support from the DARPA QuIST (MIPR 02 N699-00) program. Y.S.W. acknowledges the support of the National Research Council through the Naval Research Laboratory. Computations were performed at the ASC DoD Major Shared Resource Center.

[1] M. A. Neilson and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, U.K., 2000).

[2] P. W. Shor, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society Press, Los Alamitos, CA, 1994).

[3] L. K. Grover, in *Proceedings of the 28th Annual Symposium on the Theory of Computing* (ACM Press, New York, 1996).

[4] S. Lloyd, Science **273**, 1073 (1996).

[5] S. Lloyd, Phys. Rev. A **55**, 1613 (1997).

[6] A. Harrow, P. Hayden, and D. Leung, Phys. Rev. Lett. **92**, 187901 (2004).

[7] J. Emerson, Y. S. Weinstein, M. Saraceno, S. Lloyd, and D. G. Cory, Science **302**, 2098 (2003).

[8] A. Scott and C. Caves, J. Phys. A **36**, 9553 (2003).

[9] Y. S. Weinstein, T. F. Havel, J. Emerson, N. Boulant, M. Saraceno, S. Lloyd, and D. G. Cory, J. Chem. Phys. **121**, 6117 (2004).

[10] F. Haake, *Quantum Signatures of Chaos* (Springer, New York, 1992).

[11] T. Gorin and T. H. Seligman, Phys. Lett. A **309**, 61 (2003).

[12] G. Teklemariam, E. M. Fortunato, C. C. Lopez, J. Emerson, J. P. Paz, T. F. Havel, and D. G. Cory, Phys. Rev. A **67**, 062316 (2003).

[13] Y. S. Weinstein and C. S. Hellberg, Phys. Rev. A **69**, 062301 (2004).

[14] E. P. Wigner, Ann. Math. **62**, 548 (1955); **65**, 203 (1957).

[15] See T. Guhr, A. Müller-Groeling, and H. A. Weidenmüller, Phys. Rep. **299**, 189 (1998), for a comprehensive review.

[16] F. J. Dyson, J. Math. Phys. **3**, 140 (1962).

[17] M. L. Mehta, *Random Matrices* (Academic Press, New York, 1991).

[18] K. Zyczkowski and M. Kus, J. Phys. A **27**, 4235 (1994).

[19] Y. S. Weinstein and C. S. Hellberg, e-print quant-ph/0405053.

[20] K. Zyczkowski, *Chaos—The Interplay Between Stochastic and Deterministic Behavior, Proceedings, Karpacz, Poland 1995*, edited by P. Garbaczewski, M. Wolf, and A. Weron (Springer Berlin, 1995).

[21] S. Wolfram, *A New Kind of Science* (Wolfram Media, Champaign, IL, 2002).

[22] S. Lloyd, Science **261**, 1569 (1993).

[23] J. Watrous, in *Proceedings of the 36th IEEE Symposium on the Foundations of Computer Science*, (IEEE Computer Society press, Los Alamitos, CA, 1995), p. 528.

[24] S. C. Benjamin, Phys. Rev. A **61**, 020301(R) (2000).

[25] G. K. Brennen and J. E. Williams, Phys. Rev. A **68**, 042311 (2003).